Getting the Best Bang for the Buck with Managed Security Providers

Wade Woolwine
Manager, Managed Defense
Mandiant

Wade Woolwine

- Managed Defense
- Application Security
- Network Monitoring
- Development

Why Service Providers?

- Provide bundled technology and experts
- Lower cost capabilities
- BIG names doing work for you

- IT Security Outsourcing is on the rise year over year
  - Forecast: 49.1 Billion in 2015!!! (Source: Gartner)

Why Build Relationships?

- $$$$

Provider Selected. What Now?

- Your Existing Policies
- Contracts, Statements of Work, and Legal – OH MY!
- Knowing Your Capabilities / Knowing Their Capabilities
- Your Technology / Their Technology
- Executive Support

- Managing Change

Kick Off!

- Initial Kick Off Contact
  - Their Points of Contact
  - Your Points of Contact
  - Service Delivery Processes
  - Deliverables
  - SLAs!
- Technical Follow Up
  - Do you Have the Right People at the Table?
  - Communicating Your Architecture, Assets, and Processes
  - Understanding Their Technology and Processes

Technology Deployment

- Success is on YOU!
  - Know Your Architecture
  - Know Your Environment
  - DEPLOY EVERYWHERE!
- Validating Technology Deployment
- Incident and Disaster Recovery Dry Run

Ongoing Communication

- Managed Service Status
- Technology Status
- Service Reviews
- Communicating Changes
- Managed Service Feedback

In the Heat of the Moment. BE READY!

- Incident Reports
  - Low Severity
  - Medium Severity
  - High Severity
- Incident Response
  - Initial Response
  - Ongoing Communications
  - Remediation
- SLA miss / Service Delivery Failure

Tales from the Battlefield. WINS!

- Identification and Removal of Compromised Assets
- Rapid Implementation of Network Blocks
- Quick Approvals
- Complimentary Capabilities
- Collaboration
- Communications
- Executive Support

Tails from the Battlefield. FAILS!

- Lack of Engagement
- Assumptions
- Knowledge Gaps
- Too Much Outsourcing
- Lack of Preparedness
- Lack of Internal Communication
- Lack of External Communication
- Lack of Process
- Incomplete Technology Deployment

How Mandiant Managed Defense Does It.

- Kick Off Call
- Technology Deployments
- The Threat Assessment Manager
- The Service
  - Threat Monitoring
  - Incident Response
- What we Expect from our Customers

DO IT RIGHT. DO IT NOW.

- THANK YOU!
  - Questions?

- Managed Defense Demos Available in the Lobby.